Fundamentos dos protocolos internet

www.4linux.com.br

Sumário

Índice de tabelas

Índice de Figuras

Capítulo 1

Fundamentos dos protocolos internet

1.1. Objetivos

- Máscaras de redes;
- dotted quad;
- Diferenças entre IPv4 e Ipv6;
- Rota padrão;
- Portas;
- UDP, TCP e ICMP;
- Comandos uteis.

1.2. Mãos a obra

Máscaras de redes

Uma rede de computadores pode ser definida por vários computadores interligados entre si. Quando essa rede abrange uma área pequena é chamada de LAN, onde usuários trocam informações como arquivos e mensagens, e acessam recursos compartilhados por um servidor. É chamada de WAN quando temos uma abrangência geograficamente maior, exemplo a internet.

Como eu identifico em qual rede meu micro esta?

É nessa hora que entra o papel da mascara de rede, onde tem a função de separar em um IP a parte correspondente à rede, subrede e aos hosts.

Vamos á prática: use o comando ifconfig eth0 para exibir a sua mascara!

 # ifconfig eth0

```
eth0      Link encap:Ethernet  Endereço de HW 08:00:27:71:33:b0
          inet end.: 192.168.200.10  Bcast:192.168.200.255  Masc:255.255.255.0
          endereço inet6: fe80::a00:27ff:fe71:33b0/64 Escopo:Link
          UP BROADCASTRUNNING MULTICAST  MTU:1500  Métrica:1
          RX packets:218052 errors:0 dropped:0 overruns:0 frame:0
          TX packets:163986 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:69807508 (66.5 MiB)  TX bytes:64823946 (61.8 MiB)
```

Veja no exemplo o campo "Masc:255.255.255.0" onde exibe a mascara de rede. Além desta mascara temos outras separadas por classes.

Máscara de rede classe A: 255.0.0.0
Máscara de rede classe B: 255.255.0.0
Máscara de rede classe C: 255.255.255.0

A utilização e cada classe vai depender da dimensão potencial de sua rede.

Veja a lista abaixo:

Classe A: 10.0.0.0 até 10.255.255.255 (16.777.216 IPs possíveis)
Classe B: 172.16.0.0 até 172.31.255.255 (65.536 IPs possíveis)
Classe C: 192.168.0.0 até 192.168.255.255 (256 IPs possíveis)
Classe D: 239.0.0.0 até 239.255.255.255 (Multicast)

O endereço IP de cada maquina (host) é usada para a comunicação entre elas na rede, e o formato X.X.X.X de cada IP vem do termo inglês dotted quad (separados por pontos em grupos de números decimais correspondentes a cada 8 bits do número IP).

```
Exemplo no formato decimal: 192.168.200.10
Exemplo no formato binário: 11000000.10101000.11001000.00001010
```

Os IPs de cada classe são chamados de privados e não validos na internet. Os IPs públicos são usados por clientes e servidores para o acesso a internet, e são obtidos através de links de radio, conexão ADSL, 3G, cable modems, entre outras.

Um exemplo real e simples, seria um servidor usado para compartilhar o acesso a internet para computadores da rede local. A maquina servidor tem que ter no minimo 2 placas de redes, a primeira interface de rede (eth0) configurada com IP publico e a segunda interface de rede (eth1) configurada com IP privado.

A comunicação entre as maquinas que estão na LAN e as maquinas que estão na WAN, é feita usando uma técnica chamada NAT (Network Address Translation). Que faz a tradução dos endereços IPs e portas TCP da rede local para a Internet.

O IP trabalha no formato padrão de 32bits (quatro octetos de bits) e é conhecido como IPV4. Como a quantidade de empresas e hosts vem crescendo, foi criado um outro padrão chamado IPV6, assim disponibilizando uma quantidade maior de IPs.

O IPV6 é capaz de gerar $3,4x10^{38}$ endereços contra 2^{32} endereços do IPV4. Os endereços IPV6 são escritos com oito grupos de 4 dígitos hexadecimais.

Exemplo:

```
2001:0db8:85a3:08d3:1319:8a2e:0370:7344
```

Os computadores que estão na LAN precisam uma rota até a WAN, e isso é feito através do gateway da rede. O endereço IP atribuído á interface eth1 da maquina servidor é usada como rota padrão para todos os computadores da rede local. Veja um exemplo prático digitando o comando route -n em uma maquina local.

```
# route -n
```

```
Tabela de Roteamento IP do Kernel
Destino         Roteador        MáscaraGen.     Opções Métrica Ref    Uso Iface
192.168.200.0   0.0.0.0         255.255.255.0   U      0       0        0 eth0
0.0.0.0         192.168.200.254 0.0.0.0         UG     0       0        0 eth0
```

Em nosso exemplo a rota padrão da maquina local é 192.168.200.254 (Roteador), que ser resume no IP da interface eth1 da maquina servidor.

O que torna possível a comunicação entre os serviços na rede?

Os recursos disponíveis a partir de um computador servidor na rede, são chamados de serviços, e são transmitidos através de protocolos de rede.

Cada protocolo tem uma porta especifica determinada pela IANA (Internet Assigned Numbers Authority).

Veja a lista completa de portas no site:

http://www.iana.org/assignments/port-numbers

No Linux é possível ver a lista completa através do arquivo /etc/services:

```
# vim /etc/services
```

As portas de cada serviço são campos de 16 bits, existindo no máximo 65535. Cada serviço tem sua porta padrão, que pode ser alterada conforme sua necessidade. As portas trabalham usando os protocolos TCP e UDP. Veja na tabela abaixo as principais portas de serviços:

Porta	Serviço
20	FTP (Porta de dados)
21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
119	NNTP (Usenet)
139	Netbios

143	IMAP
161	SNMP
443	HTTPS
465	SMTPS
993	IMAPS
995	POP3S

Qual a diferença entre os protocolos?

Na prática quando uma maquina se comunica com a outra, elas utilizam o protocolo TCP/IP para transferir dados. O TCP/IP é formado por um grande conjunto de diferentes protocolos e serviços de rede.

O nome vem do protocolo TCP usado para transporte, que executa funções garantindo que os dados sejam entregues de uma maneira confiável. O IP que é um protocolo de endereçamento que fornece uma maneira para identificar cada máquina da rede.

Ainda na parte de protocolos temos o UDP (User Datagram Protocol) usado no transporte de dados entre hosts, porém não fornece garantia de entrega e nem verificação de dados. O UDP pode ser muito mais rápido, por não fazer verificações e por não estabelecer sessões.

Um exemplo simples de comunicação pode ser feita através do comando ping:

 # ping 192.168.200.254 -c4

```
PING 192.168.200.254 (192.168.200.254) 56(84) bytes of data.
64 bytes from 192.168.200.254: icmp_seq=1 ttl=64 time=7.85 ms
64 bytes from 192.168.200.254: icmp_seq=2 ttl=64 time=0.235 ms
64 bytes from 192.168.200.254: icmp_seq=3 ttl=64 time=0.214 ms
64 bytes from 192.168.200.254: icmp_seq=4 ttl=64 time=0.194 ms

--- 192.168.200.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
rtt min/avg/max/mdev = 0.194/2.123/7.850/3.306 ms
```

Em nosso exemplo a maquina local usou o comando ping para se comunicar com o gateway da rede. O uso da flag -c4 serve para o ping parar após o envio de 4 pacotes. O ping usa o protocolo ICMP que permite a comunicação entre roteadores e hosts, assim identificando e relando o estado de funcionamento da rede.

A comunicação entre maquinas na rede pode ser feita de varias maneiras, um exemplo foi através do comando ping para verificar o funcionamento da rede. Existem outros comandos que uteis que podem ser usados na rede, vamos a prática:

Ftp – Comando usado para transferir arquivos a partir de um site de rede remota. Exemplo:

 # ftp ftp.conectiva.com.br

```
Connected to ftp.conectiva.com.br.
220 Conectiva FTP server
Name (ftp.conectiva.com.br:roberto): anonymous
331 Anonymous login ok, send your complete email address as your password.
Password:
230 Anonymous access granted, restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Em nosso exemplo o usuário anonymous foi usado para ter acesso ao host remoto. Você pode usar comandos para por exemplo listar arquivos (ls), visualizar o diretório atual (pwd), trocar de diretório (cd), fazer download (get), entre outros. Use o comando quit para fechar a conexão ftp.

Telnet - Comando usado para comunicação entre hosts usando protocolo TELNET, além de permitir o acesso remoto a um outro host. A comunicação via telnet é feita usando texto plano, assim sendo substituído por SSH, onde o conteúdo é criptografado antes de ser enviado. Exemplo:

 # telnet 192.168.200.254

```
Trying 192.168.200.254...
Connected to 192.168.200.254.
Escape character is '^]'.
debian login: Connection closed by foreign host.
roberto@servermc:~$ telnet 192.168.200.254
Trying 192.168.200.254...
Connected to 192.168.200.254.
Escape character is '^]'.
debian login: aluno
Password:
```

Sempre use o SSH para acesso remoto!!!

Mesmo que o telnet não tenha segurança, ele ainda é mantido e pode ser muito útil quando você precisa testar o funcionamento de um servidor de email. Veja os 2 exemplos:

 # telnet localhost 25

 # telnet localhost 110

*D*ig – Comando usado para interrogar servidores de nome, ele realiza pesquisas de DNS e exibe as respostas que são devolvidos a partir do servidor. Exemplo:

 # dig terra.com.br.

```
; <<>> DiG 9.5.1-P3 <<>> terra.com.br.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11612
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;terra.com.br.                  IN      A

;; ANSWER SECTION:
terra.com.br.           7043    IN      A       200.154.56.80

;; AUTHORITY SECTION:
terra.com.br.           7043    IN      NS      ns2.terra.com.br.
terra.com.br.           7043    IN      NS      ns1.terra.com.br.

;; Query time: 31 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Jun 21 20:48:56 2010
;; MSG SIZE  rcvd: 82
```

Em nosso exemplo o dig buscou informações sobre o terra, veja em “ANSWER SECTION” que o host tem IP 200.154.56.80.

Como eu posso testar o DNS reverso de um host?

Simples! Use o dig com a flag -x e o IP do host apresentado. Vamos a prática:

 # dig -x 200.154.56.80

```
; <<>> DiG 9.5.1-P3 <<>> -x 200.154.56.80
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44426
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;80.56.154.200.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
80.56.154.200.in-addr.arpa. 172426 IN   PTR     www.terra.com.br.

;; AUTHORITY SECTION:
56.154.200.in-addr.arpa. 172426 IN      NS      ns1.terra.com.br.
56.154.200.in-addr.arpa. 172426 IN      NS      ns2.terra.com.br.

;; Query time: 19 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Jun 21 20:54:59 2010
;; MSG SIZE  rcvd: 110
```

Veja que o DNS reverso esta OK!

Traceroute – Comando usado para fazer um rastreio de rota como o próprio nome diz. Ele consegue obter o caminho que um pacote atravessa por uma rede de computadores até chegar ao destinatário utilizando o protocolo ICMP. Exemplo:

 # traceroute 4.2.2.2

Tracepath – Comando bastante similar ao traceroute, mas mostra o pmtu do caminho percorrido.

Para instalar no Debian:

 # aptitude install iputils-tracepath

Para instalar no RedHat:

 # yum install iputils

Para instalar no OpenSuse:

```
# zypper install iputils
```

```
# tracepath 4.2.2.2
```

A MTU (Unidade Máxima de Transmissão) é o tamanho do maior datagrama que pode ser enviado através de uma rede. O termo PMTU (Path MTU) será sempre igual ao menor MTU ao longo de todo o caminho que o datagrama deve viajar.

Capítulo 2

Gerenciando

2.1. Objetivos

- *Cenário - Utilizando placa de rede virtual.*

2.2. Troubleshooting

Como eu faço para compartilhar minha internet da maquina real para minha maquina virtual, com apenas uma interface de rede?

Veja uma situação real e muito comum, onde você possui apenas uma interface de rede eth0 co IP publico e precisa compartilhar a internet para sua maquina virtual.

Você simplesmente poderia comprar uma outra placa de rede, assim teria a eth0 para WAN e eth1 para LAN. Mas é possível economizar dinheiro e tempo adicionando uma placa de rede virtual. Isso pode ser feito de 2 maneiras na maquina real, vamos a prática:

```
# ifconfig eth0:0 192.168.200.254
```

ou

```
# ifconfig eth0 add 192.168.200.254
```

```
eth0      Link encap:Ethernet  Endereço de HW 00:0f:ea:de:15:e2
          inet end.: 187.21.92.7  Bcast:187.21.95.255  Masc:255.255.240.0
          endereço inet6: fe80::20f:eaff:fede:15e2/64 Escopo:Link
          UP BROADCASTRUNNING MULTICAST  MTU:1500  Métrica:1
          RX packets:756382 errors:0 dropped:0 overruns:0 frame:0
          TX packets:427132 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:1031455710 (983.6 MiB)  TX bytes:42967035 (40.9 MiB)
          IRQ:220 Endereço de E/S:0x8000

eth0:0    Link encap:Ethernet  Endereço de HW 00:0f:ea:de:15:e2
          inet end.: 192.168.200.254  Bcast:187.21.95.255  Masc:255.255.240.0
          UP BROADCASTRUNNING MULTICAST  MTU:1500  Métrica:1
          IRQ:220 Endereço de E/S:0x8000
```

Para apagar use o comando:

```
# ifconfig eth0 del 192.168.200.254
```

Pronto agora você pode usar uma regra de iptables para compartilhar a internet, e caso queira deixar no boot, configure a placa virtual no arquivo /etc/network/interfaces